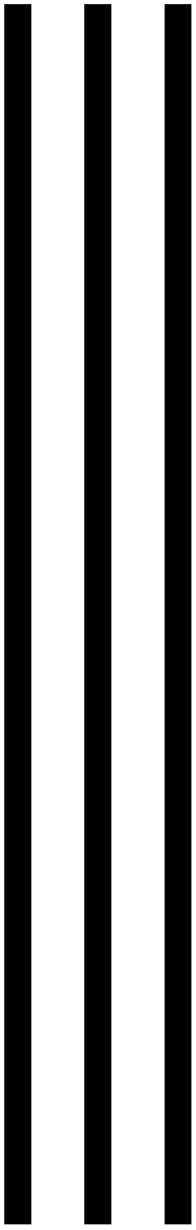

U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

SECURITY OVER THE INFORMATION TECHNOLOGY RESOURCES AT THE FOOD SAFETY AND INSPECTION SERVICE

Report No.
24099-1-FM
August 2003

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: AUG 11 2003

REPLY TO
ATTN OF: 24099-1-FM

SUBJECT: Security Over the Information Technology Resources at the Food Safety and Inspection Service

TO: Garry L. McKee
Administrator
Food Safety and Inspection Service

This report presents the results of our audit of the Security Over Information Technology Resources at the Food Safety and Inspection Service (FSIS). The report identifies internal control weaknesses in FSIS' ability to protect its critical information technology resources. While the FSIS has substantial actions underway, additional measures are needed to further strengthen FSIS' information technology security. FSIS has implemented plans to correct these areas of concern.

Your response to our draft report is included in its entirety in exhibit A, with excerpts incorporated into the findings and recommendations section of the report. Based on the information provided in the response, we have reached management decision for all recommendations. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us during this audit.

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

SECURITY OVER THE FOOD SAFETY INSPECTION SERVICE'S INFORMATION TECHNOLOGY RESOURCES

AUDIT REPORT NO. 24099-1-FM

RESULTS IN BRIEF

We identified weaknesses in the Food Safety Inspection Service's (FSIS) ability to adequately protect its information technology (IT) resources from potential disruptions. IT security related weaknesses were found at the FSIS Headquarters (HQ) office, including vulnerabilities related to FSIS' IT equipment and its ability to continue processing in case of unscheduled disruptions. Specifically, we found the following.

- Our vulnerability scans of selected FSIS systems disclosed weaknesses that may be exploited both internally and externally from the Internet. FSIS officials stated that the results of their self-completed scans were provided to the various system administrators for correction; however, FSIS had maintained no formal records which identified vulnerabilities that were fixed or that identified vulnerabilities that cannot be fixed for various reasons and the processes in place for mitigating these risks. Further, FSIS did not have a standard security policy in place to protect its networks or ensure that identified vulnerabilities were corrected timely. As a result, FSIS' systems are vulnerable to cyber-related attacks, jeopardizing the integrity and reliability of its data. The results of our scans were provided to the responsible FSIS personnel who immediately began taking corrective actions on the vulnerabilities.

- FSIS had not adequately protected physical access to its HQ computer facility to allow only users who need access in order to perform their duties. FSIS uses its computer room for the storage of excess computer hardware, which requires the need for additional employees to have access to that room. Also, physical security controls concerning fire suppression, entry door security, security planning and offsite storage of backup tapes need to be improved. In addition, FSIS does not have an adequate process for ensuring that user identifications, for personnel who no longer need access to the major applications, are removed timely. FSIS officials informed us that they did not have the resources to implement and enforce such controls.

As a result, FSIS critical data are at an increased risk of unauthorized disclosure, modification or deletion.

- Database administrators (DBA) were allowed to make changes to FSIS data without following up with appropriate personnel to verify the validity of the change. This occurred because FSIS had not implemented a formal process for its DBAs to follow when making changes to the various databases maintained at the FSIS HQ. Further, FSIS had not established a supervisory review and approval process to ensure that only authorized changes were made to the databases. While the DBAs informed us that they believed that their actions were appropriate, they did not understand what impact their actions had on the integrity of the databases. A lack of sufficient controls over database changes and authorizations could result in misreporting critical data to FSIS management, Congress, and other agencies that use such data.

- FSIS has not completed all security plans required by Office of Management and Budget (OMB) Circular A-130. Further, for those that have been completed, FSIS has not periodically updated those plans to reflect current conditions. This occurred because FSIS does not have a formal process in place to ensure that security plans are prepared and kept current for each of its general support systems or to ensure that its major applications have been certified and authorized for processing. FSIS officials informed us that they had not made these security reviews a priority and had not been given the personnel and other resources to complete these reviews. Without current and complete security plans and security reviews of major applications, FSIS cannot ensure that controls over its IT resources, including many mission-critical systems, are adequate.

- FSIS had not developed a formal plan to ensure the recovery and continuity of operations in the event of a disaster. FSIS officials recognized the need to prepare plans to address business continuity, but officials informed us that this task had yet to be a priority. FSIS officials further cited a lack of personnel and other resources to complete these plans. As a result, FSIS cannot be assured that it can quickly and effectively resume operations in the event of a disaster or other service disruption.

- FSIS had not implemented a standard system development life cycle (SDLC) process for managing its application development and change control process. FSIS does not maintain formal project plans, change control forms, approvals, test plans, or testing results. FSIS officials agreed that a standard SDLC was not in place, but said that funding

had not been approved that would allow them to establish a formal SDLC. We also reported FSIS' lack of adequate testing and documentation of testing results in Audit Report No. 50099-21-FM, "Review of the Year 2000 Conversion Process - Validation Phase," issued in September 1999. Without a formal SDLC process and adequate documentation, it is not possible to assess whether systems under development and systems undergoing modification are properly approved, contain all needed security features, and are properly authorized before modifications are made.

We believe that the findings in this report should be included in FSIS' Federal Managers' Financial Integrity Report until corrected.

KEY RECOMMENDATIONS

We recommended that FSIS take appropriate immediate action to address the conditions noted, including the following:

- Take the necessary corrective actions on the high and medium-risk vulnerabilities identified.

- Develop a formal process for conducting security scans which includes procedures to ensure vulnerabilities are reviewed and corrective actions documented in a timely manner.

- Develop a formal process for granting physical access to the computer facilities ensuring that only employees who need access to the computer room for the performance of their duties are allowed access.

- Develop a formal process to ensure that only authorized changes are made to databases and require full documentation of the need for each change with management's review and approval.

- Update the security plan for the computer facility to reflect the current operating environment and to address all the required security actions.

- Prepare and periodically update comprehensive and system specific contingency plans that address protection for information resources and recovery procedures, including offsite storage requirements.

- Adopt and follow a standard system development life cycle process for all major applications.

During the course of our review, FSIS officials cited a lack of sufficient personnel and other resources as a cause to several issues we identified. If FSIS is unable to implement our recommendations as presented, FSIS

needs to implement compensating controls to minimize the risk to its systems and network, or engage the help of the Office of the Chief Information Officer to plan a course of action to mitigate those risks.

AGENCY RESPONSE

FSIS agreed with the findings and recommendations in the report. FSIS has taken or planned significant actions to correct the weaknesses we identified.

OIG POSITION

We concurred with FSIS' actions and have reached management decision on all recommendations.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Food Safety and Inspection Service (FSIS) of the U.S. Department of Agriculture (USDA) assures that meat, poultry, and egg products moving in interstate and foreign commerce for use as human food are safe, wholesome, and accurately labeled and packaged. FSIS also informs the public about food safety issues. Historically, USDA agencies have separately addressed their respective information technology (IT) security and infrastructure needs. These isolated approaches have resulted in a broad array of technical and physical solutions that do not assure that complete Department-wide security is obtained.

FSIS protects the public health by regulating meat, poultry, and egg products, which includes: all raw beef, pork, lamb, chicken and turkey, as well as processed meat and poultry products, including hams, sausage, soups, stews, pizzas, and frozen dinners.

Under the Federal Meat Inspection Act, the Poultry Products Inspection Act, and the Egg Products Inspection Act, FSIS inspects all meat, poultry and egg products sold in interstate commerce and re-inspects imported products to ensure they meet U.S. food safety standards. More than 8,100 inspection personnel verify that regulations regarding food safety and other consumer protection concerns such as labeling are met in nearly 6,500 meat, poultry, and egg processing plants. In slaughter plants, inspection involves examining (before and after slaughter) birds and animals intended for use as food. In egg processing plants, inspection involves examining (before and after breaking) eggs intended for further processing and use as food.

The Office of Management, Automated Information Systems Division, Information Systems Security Program Manager (ISSPM) is responsible for the overall IT security within FSIS. To facilitate this, FSIS has designated Deputy ISSPMs in each of its program areas.

OBJECTIVES

Our primary audit objectives were to determine (1) if FSIS had adequate security measures in place to protect sensitive data against cyber based penetration attempts; (2) if FSIS had adequate logical and physical access controls to protect

computer resources against unauthorized modification, disclosure, loss, or impairment; and (3) if FSIS had adequate controls over the modification of application and system software programs to ensure that only authorized modifications are implemented.

SCOPE

This audit was a review of the FSIS Headquarters (HQ) IT security. We reviewed controls established to ensure the integrity of information security over the systems located in Washington, D.C., and the controls established to ensure security over systems located at FSIS field sites.

Our audit was performed from February through August 2002. We conducted our review at the FSIS HQ in Washington, D. C. Our review included vulnerability scans that were conducted on various hardware platforms and network components.

We conducted this audit in accordance with Government Auditing Standards.

METHODOLOGY

To accomplish the audit objectives, we performed the following procedures.

- Reviewed IT policies and procedures relating to various security aspects of FSIS.
- Interviewed responsible FSIS security officials and other personnel responsible for managing IT resources.
- Performed vulnerability scans of various servers and routers.
- Reviewed departmental and agency security procedures and directives.
- Reviewed disaster recovery and contingency planning efforts.
- Reviewed agency policies and procedures concerning change controls for major applications.
- Reviewed agency security plans for general support systems and major applications.
- Reviewed agency Government Performance and Results Act reports and interviewed pertinent personnel.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1 | VULNERABILITIES EXPOSE FSIS' SYSTEMS TO RISK

FINDING NO. 1

Our vulnerability scans of selected FSIS systems disclosed weaknesses that may be exploited both internally and from the Internet. FSIS officials stated that the results of their self-completed scans were provided to the various system administrators for correction; however, FSIS had maintained no formal records that identified vulnerabilities that were fixed or that identified vulnerabilities that cannot be fixed for various reasons and the processes in place for mitigating these risks. Further, FSIS did not have a standard security policy in place to protect its networks or ensure that identified vulnerabilities were corrected timely. As a result, FSIS' systems are vulnerable to cyber-related attacks, jeopardizing the integrity and reliability of its data.

To conduct our assessment we used a commercially available software product that was designed to test for over 1,000 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP)[1]. Our vulnerability scans provide the agency with a snapshot of the vulnerabilities present at the time of the scan. The results of our scans were provided to the responsible FSIS personnel who immediately began taking corrective actions on the high and medium vulnerabilities.

TCP/IP System Vulnerabilities

Our assessments revealed 6 high and 67 medium-risk vulnerabilities. We reported the weaknesses directly to agency management to ensure timely corrective actions. In addition, we identified over 250 low-risk vulnerabilities, many of which, while not critical to system security, can be an indicator of the need for better system administration. FSIS had the identical scanning tool we used, but the vulnerabilities identified by FSIS' internal scans preceding our reviews had not been corrected at the time of our review.

[1] TCP/IP is the suite of communication protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

Detailed below are examples of the high-risk[2] vulnerabilities disclosed during our scans of the various FSIS systems.

- Various versions of a protocol were identified that are vulnerable to a wide range of attacks. This protocol, if left uncorrected, could allow an attacker to gain control over FSIS' network resources.

- An operating system service was identified as having contained a programming error which could potentially allow complete control over the system.

- An operating system software version, currently running, could allow a remote attacker to gain full administrative access over the device.

On one specific instance, FSIS had conducted scans of some of its servers on April 2, 2002, using the same scanner program that we used. We compared the results of our scans to those conducted by FSIS to determine the extent of corrective actions initiated by FSIS. Our review disclosed that the vulnerabilities were nearly identical between the scan results, indicating that FSIS had not initiated corrective actions on the vulnerabilities they previously identified.[3] FSIS personnel said they do not have a formal process in place for correcting the vulnerabilities identified during the scans. They said the results of the scans are provided to the various system administrators for correction; however, there are no formal records kept which identify vulnerabilities that were fixed or identify vulnerabilities that cannot be fixed for various reasons.

These vulnerabilities, if left uncorrected, could allow unauthorized users access to critical and sensitive FSIS programs and systems. We met with FSIS officials to discuss the results of our assessments and the procedures necessary to mitigate the vulnerabilities found. They concurred with our findings and were actively working to correct the vulnerabilities identified.

We also found that FSIS had not implemented firewalls to provide additional security for its network. FSIS personnel said they are in the process of implementing firewall security, but this had not been completed at the time of our review.

---

[2] High-risk vulnerabilities are those that provide access to the computer, and possibly the network of computers. Medium-risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low-risk vulnerabilities are those that provide access to sensitive, but less significant network data.

[3] No high-level vulnerabilities existed on these systems. However, medium-level vulnerabilities should also be corrected to the extent possible.

RECOMMENDATION NO. 1

Ensure all necessary corrective actions are completed on all high and medium-risk vulnerabilities identified during our audit.

Agency Response

FSIS stated that it has completed corrective actions on all 6 high-risk vulnerabilities identified during the audit. Action was also completed on 62 of the 73 medium vulnerabilities, with 11 still unresolved. The Agency's progress in addressing the vulnerabilities is evident when a comparison is made between the original scan report and a recent scan. The Agency will institute fixes for the remaining 11 unresolved medium vulnerabilities. A report detailing the Agency's corrective actions to resolve these 11 will be prepared by September 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 2

Develop a formal process for conducting security scans of the servers and network equipment that include procedures to ensure vulnerabilities are reviewed and that corrective actions are documented.

Agency Response

FSIS stated that it has instituted bi-weekly [redacted] inspections. The scans allow FSIS IT personnel to regularly perform audits and assess the network parameters and stay cognizant of any potential security misconfigurations and anomalies. The bi-weekly inspections allow FSIS to take the necessary corrective actions before the network is compromised. Patches that are approved for use on FSIS operating systems and applications are usually implemented within three weeks after the scan dates. Patches that cannot be applied will be documented as to why they were not approved and installed.

Additionally, FSIS purchased an intrusion prevention software package to help protect the integrity of FSIS' applications and operating systems. The software proactively protects enterprises against known and unknown security risks. Unlike existing FSIS security solutions that are attack-centric and reliant on databases of known attack signatures, software is application-centric, focusing on the behavior of FSIS critical computer applications.

Subsequent discussions with FSIS officials disclosed that the bi-weekly scanning process has been in place since April 11, 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 3

Ensure that the ongoing process of installing firewall security is completed timely.

Agency Response

FSIS stated that it is in the process of implementing firewall security. FSIS will establish controls to periodically review the firewall configuration to ensure that it is kept current and that user accounts on the firewall system are kept to a minimum and are properly disabled or removed when not needed. FSIS will complete the firewall security installation by December 2003.

OIG Position

Management decision has been reached on this recommendation.

CHAPTER 2	FSIS NEEDS TO IMPROVE THE PHYSICAL AND LOGICAL ACCESS CONTROLS OVER ITS NETWORK AND CRITICAL DATABASES

FINDING NO. 2

FSIS NEEDS TO IMPROVE ITS PHYSICAL AND LOGICAL ACCESS CONTROLS TO ITS NETWORK RESOURCES

FSIS had not adequately controlled physical access to its HQ computer facility to allow only users who need access in order to perform their duties. FSIS uses its computer room for the storage of excess computer hardware, which requires the need for additional employees to have access to that room. Also, physical security controls concerning fire suppression, entry door security, security planning and offsite storage of backup tapes need to be improved. In addition, FSIS does not have an adequate process for ensuring that user identifications (ID), for personnel who no longer need access to the major applications, are removed timely. Separation reports of FSIS personnel are not routinely distributed to responsible personnel to ensure employee accesses are removed timely. FSIS officials informed us that they did not have the resources to implement and enforce such controls. As a result, FSIS critical data are at an increased risk of unauthorized disclosure, modification or deletion.

Departmental Manual (DM) 3140-1.6, "ADP Security Manual," (part 6 of 8), Appendix D, Section 6c, requires security staff to remove employee user identifications and passwords when the employee is no longer with the agency. Part 9, "Security Plans," requires the agency to submit an annual security plan or security plan update by March 31 of every year. And part 15, "Software and Data Security Standards," requires that logs be maintained to record the location of files and equipment that have been removed from the facility.

Computer Facility Security

FSIS does not have a formal process in place for granting access to its computer room. Employees are not required to complete any type of form requesting access to the computer room indicating why they need access and requiring supervisory approval of the need. FSIS provided a list of 32 employees who had unescorted access to the computer room. The list included help desk employees, database administrators, and application development personnel. FSIS personnel said the help desk employees needed access to the computer room because the computer room was also used to store various pieces of hardware the help desk personnel

needed to access. FSIS did not have a formal process in place for documenting and approving access needs; therefore, we were not able to determine the specific reasons why all of the 32 people required unrestricted access to the computer room. Through interviews, we did confirm that at least one person from the Program Application Systems Branch did not need unrestricted access to the computer room. FSIS needs to restrict physical access to its computer facilities to only systems administrators and security personnel who have responsibilities for maintaining those systems.

In addition, our walkthrough of the computer room disclosed that the halon fire suppression system had not been serviced in nearly 3 years. We were informed that this was an oversight and immediate corrective action was taken by FSIS. We also found that the computer room entry door, although secured by a cipher lock, had the door hinges located on the outside of the door accessible from the hallway. Anyone could easily by-pass the cipher lock control by removing those door hinges.

We also found that FSIS does not have a current security plan in place for the computer room operations. We were provided a draft general support plan for the FSIS Enterprise Network, dated March 2002. However, some of the computer equipment described in the plan is no longer used by FSIS. In addition, the plan referenced a risk assessment review to be performed by the National Security Agency, which was to take place during fiscal year (FY) 2000. The plan also identified various security actions such as training, authorized processing, review of security controls, design review and testing and incident response capability as "PLANNED" to be done. However, none of these have been accomplished.

FSIS has an offsite storage location for its backup tapes; however, FSIS has no written procedures for performing the tape backups and no inventory of tapes kept offsite. Our review identified tapes that, according to FSIS personnel, should have been at the offsite facility. FSIS personnel said that this was probably just a labeling error; however, FSIS had no backup tape labeling standard in place. Finally, we found that the current backup tapes were simply stored in a desk drawer with many out-of-date backup tapes until they were transported to the off site storage facility.

Application Access Controls

FSIS personnel are provided access to its network by the Electronic Mail Coordinators (EMC) located throughout the various FSIS program areas. The EMCs can request all types of account changes, modify user

information, add or delete users, unlock accounts and reset passwords. Managers of FSIS' major applications are responsible for providing FSIS employees with their needed access. However, neither the EMCs nor the application managers routinely receive separation reports of terminated employees. In addition, FSIS was not using the logs prepared by the application's access control software to identify unauthorized or unusual access attempts, nor was any person assigned the responsibility of reviewing those access control software logs.

We obtained a listing of separated employees from the FSIS Human Resources Division, for the period March 2000 through March 2002, and a listing of active employees from USDA's National Finance Center. Our comparison of these lists to current user IDs on selected FSIS applications identified at least 90 user IDs belonging to former employees. Interviews with the various EMCs and the individual application managers confirmed that they were not routinely provided a list of separated employees.

FSIS also uses access control software for tracking access to its general network environment. This software tracks security and auditing related events and stores them in a security event log. This software also can be used to filter specific security events but FSIS was not using this option. We identified seven system administrators that have authority to review the security event logs, but none have been specifically assigned responsibility for reviewing the logs.

RECOMMENDATION NO. 4

Develop a formal process for granting physical access to the HQ computer facility that includes requiring the completion of an access request form identifying the reason the access is needed and requiring supervisory approval of the need.

Agency Response

FSIS informed us that it will develop a formal process for granting access to the HQ computer facility that includes requiring the completion of an access request form identifying the reason the access is needed and requiring supervisory approval of the need. The written process will include the procedures for authorizing approval for access to the HQ computer facility. The form will provide a general description of the grantee's work function requiring access to the computer facility. For efficiency, a single form will be used to cover continuing activities that require recurring access to the facility. FSIS will complete the development of the formal process and form by December 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 5

Ensure that only employees who need access to the computer room for the performance of their duties are allowed unrestricted access.

Agency Response

FSIS stated that it is in the process of removing and relocating spare equipment that was being stored in the computer facility to a separate secure location to limit access to the computer facility. In addition, FSIS will install a card key access system that will track individuals entering the computer facility. Only employees requiring access to the computer room for the performance of their duties will be allowed unrestricted access. Funds for the card key system have been committed and FSIS is making arrangements with the Department to proceed with the work. FSIS expects the new system to be operational by December 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 6

Take action to ensure that the computer room access door hinges are adequately secured.

Agency Response

FSIS stated that it has pinned the door hinges to secure them and prevent unauthorized entrance into the computer room. Three holes were drilled within the internal side of the door hinges and safety studs were inserted and welded in place to prevent removal of the hinges. Enclosure No. 2 contains a copy of the work order for this completed work.

A subsequent discussion with FSIS officials disclosed that the work was completed on April 22, 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 7

Update the security plan for the computer facility to reflect the current operating environment and to address all the required security actions.

Agency Response

FSIS stated that it will update the security plan for the computer facility. The plan will identify security actions required to maintain an adequate computer room environment. FSIS expects to have an updated security plan by May 2004.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 8

Develop and document procedures for performing tape backups that includes maintaining an inventory of tapes at the offsite storage facility and a standard tape labeling process.

Agency Response

FSIS stated that it will develop procedures for performing tape backups that includes maintaining an inventory of tapes at the offsite storage facility. The procedures will also include a process for labeling the backup tapes. FSIS will issue the procedures by May 2004.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 9

Ensure that personnel responsible for assigning and maintaining user access to the major applications are routinely provided a list of separated employees.

Agency Response

FSIS stated that it makes a concerted effort to remove separated user accounts in a timely manner. FSIS distributes to key managers a personnel list that provides information on employees that have been recently hired, separated, and transferred. Starting in July 2003, the Automated Information System Division (AISD) will be provided with a bi-

monthly list of separated or transferred employees by the Human Resources Division. The AISD personnel responsible for assigning and maintaining user access to the major applications will be provided with the list. FSIS will close user accounts of employees who no longer require access to the network within 2 business days of receipt of listing.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 10

Assign responsibilities for review of the security event history logs for all major applications and network, and identify the specific security events to be filtered for review.

Agency Response

FSIS stated that it is currently using support contractors to carry out its responsibilities for tracking the security and activity related events and storing them in a security event history log. FSIS will develop written procedures covering the process that the system administrators will use to review the security history log. The procedures will also identify the specific activity events to be filtered for review. The procedures will be developed by December 2003.

OIG Position

Management decision has been reached on this recommendation.

FINDING NO. 3

FSIS NEEDS TO IMPROVE ADMINSTRAIVE CONTROLS TO ENSURE THE INTEGRITY OF ITS DATABASES

Database administrators (DBA) were allowed to make changes to FSIS data, many times without following up with appropriate personnel to verify the validity of the change. This occurred because FSIS had not implemented a formal process for its DBAs to follow when making changes to the various databases maintained at the FSIS HQ. Further, FSIS had not established a supervisory review and approval process to ensure that only authorized changes were made to the databases. While the DBAs informed us that they believed that their actions were appropriate, they did not understand what impact their actions had on the integrity of the databases. A lack of sufficient controls over database changes and authorizations could result

in misreporting critical data to FSIS management, Congress, and other agencies that use such data.

Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources," established a minimum set of controls for agencies' automated information security programs. Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored. Further, both National Institute of Standards and Technology (NIST) Special Publication 800-12 and OMB Circular A-130, Appendix III, advocates implementation of the "least privilege" concept, granting users only those accesses required to perform their duties.

FSIS' HQ office maintains databases used to consolidate the data collected from its many field office locations. These databases are used to provide reports to various management levels, Congress, foreign governments, and other departmental agencies. FSIS has designated DBAs who have full access to the database data and can initiate data changes.

We found that the FSIS had not established a process to ensure that only authorized changes were made to the data in its databases. We interviewed the DBAs for the six major FSIS databases and found that there were no procedures in place for the DBAs to follow when making changes to their respective databases. The DBAs and their designated backup DBA can modify or delete any of the data within their databases without documenting who requested the change, management approval of the change, testing of the changes, or any second-party reviews to ensure the change was made accurately. Our discussions with DBAs indicated that it is very difficult to track where an error may have originated because the data is input from the field and may go through various district servers before residing on the HQ database.

The DBA for one of FSIS' systems said that when suspect data is identified the data is just "zeroed out" prior to preparing the report. This system captures slaughter totals and inspection summaries reported by field inspectors located in livestock and poultry slaughter establishments. This DBA stated that many times, follow up is not done to ensure that accurate changes were made to the database. Other DBAs we spoke to were able to provide some documentation for their changes such as system screen prints, but many times it was difficult to determine what had actually been changed, whether the changes were approved, and what follow up was done to ensure the change was appropriate.

Another FSIS system had an excessive number of users with DBA authority. Of the 101 total users on this system, 22 of them had DBA authority allowing them to have complete control over the database and its contents. This system, which is used by other Federal agencies, allows FSIS to track and report actions relating to volatile levels of chemicals found in slaughtered animals and egg products. FSIS needs to ensure that only those users that need this authority to conduct their jobs are granted this high-level privilege.

RECOMMENDATION NO. 11

Develop a formal process to ensure that only authorized changes are made to database data. Ensure the process requires full documentation of the need for the change and management approval and review of the change.

Agency Response

FSIS stated that it has established a Change Control Board (CCB) to oversee system changes. The CCB has the responsibility to review and approve all system and database changes. The CCB has been functioning since May 2003. The CCB Chair is responsible for ensuring that all database system changes are documented. Enclosure No. 3 contains a charter for the CCB.

FSIS will document the formal process that the CCB uses to ensure that only authorized changes are made to the database data. The formal process will be issued by December 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 12

Review the access authorities granted to the 22 individuals with DBA authority. Document these individuals need for this level of access, or remove the privilege.

Agency Response

FSIS stated that it will review the access authorities of the 22 individuals granted DBA authority. The Agency will verify that these individuals have a legitimate need for having this level of authority or remove this privilege. FSIS will complete this determination and documentation by September 2003.

OIG Position

Management decision has been reached on this recommendation.

CHAPTER 3	FSIS NEEDS TO ENSURE COMPLIANCE WITH EXISTING FEDERAL INFORMATION SECURITY REQUIREMENTS

FINDING NO. 4

FSIS NEEDS TO COMPLETE AND PERIODICALLY UDPATE ITS SECURITY PLANS

FSIS has not completed all security plans required by OMB Circular A-130. Further, for those that have been completed, FSIS has not periodically updated those plans to reflect current conditions. This occurred because FSIS does not have a formal process in place to ensure that security plans are prepared and kept current for each of its general support systems or to ensure that its major applications have been certified and authorized for processing. FSIS officials informed us that they had not made these security reviews a priority and had not been given the personnel and other resources to complete these reviews. Without current and complete security plans and security reviews of major applications, FSIS cannot ensure that controls over its IT resources, including many mission-critical systems, are adequate.

General Support Systems

OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," identifies a general support system as an interconnected set of information resources under the same direct management control that shares common functionality. Such a system can be a local area network including smart terminals that supports a branch office, and agency-wide backbone, a communications network, a departmental data processing center including its operating systems and utilities, or a shared information processing service organization.

FSIS provided security plans for two of its general support systems including the HQ computer room facility and the Financial Processing Center (FPC) in Iowa. A general support system security plan had not been prepared for the FSIS Technical Service Center (TSC) in Nebraska. However, FSIS also has computer resources located throughout its 15 district offices, has laboratories located in various parts of the country, and uses the services of the National Information Technology Center. These types of sites need to be evaluated by the FSIS to determine if general support systems security plans need to be prepared.

The plans that were provided were generally outdated and incomplete. For example, the FPC security plan which was still in a draft form showed a date of January 7, 2002. However, dates within the plan showed actions that were to be accomplished in May 1999. Various sections of the plan such as rules, training, risk assessment and management, review of security controls, authorized processing, and incident response capability all showed "Planned" without any target dates or with expired target dates, rather than identifying any type of controls actually being in place. Weaknesses associated with the undated security plan for the HQ general support systems were discussed in Finding No. 2.

An FSIS official stated that they were still in the process of identifying which general support system security plans are needed. He said currently they have identified the HQ computer facility, the FPC and the TSC as needing security plans. He agreed that both the HQ computer facility and FPC plans needed to be updated and a security plan needed to be prepared for the TSC.

Major Applications

DM 3140-1, Management ADP Security, dated July 19, 1984, Section 12, Application Certification and Recertification, states: "USDA agencies and offices will conduct periodic audits or evaluations to certify and/or recertify the adequacy of security safeguards of each sensitive operational computer application system. At a minimum, evaluations/certifications will be conducted at least every 3 years."

OMB Circular A-130, Appendix III, identifies the specific controls for securing applications. It provides the specific elements that should be included in the application security plans such as an independent review or audit of the security controls at least every 3 years, and requires that a major application should be authorized by the management official responsible for the function supported by the application at least every 3 years.

FSIS had not established a process to ensure that its major applications were certified and authorized as required by Departmental Regulations and OMB Circular A-130. FSIS identified nine major applications that required certification and authorization prior to processing; however, this had not been accomplished for any of the applications. FSIS had identified this as a discrepancy in its Information Technology Security Plan, last updated in July 2001, and stated that they "...will work to correct this deficiency within the next fiscal year."

FSIS was able to provide application security plans for seven of its nine major applications. Each of the nine applications was identified by FSIS as processing sensitive data. A review of the seven application security plans showed that some were undated and others had not been updated since 1998. Further, our review disclosed that:

- None of the plans adequately addressed contingency planning or identified that the application had been authorized for processing;

- six of the plans did not adequately address training or to the extent that the application shared information with other systems;

- five of the plans showed that a review of application controls had not been performed; and

- three of the plans did not address operating rules of the application.

Security plans for its general support and applications are one tool to ensure that FSIS has the appropriate security controls in place to protect its IT resources and the data it maintains. FSIS should establish controls to ensure that these security plans are properly completed and continually maintained throughout the lifecycle of each system.

RECOMMENDATION NO. 13	Perform an assessment to identify each of the general support systems within FSIS.

Agency Response

FSIS stated that it will identify relevant criteria and identify each of the general support systems within FSIS by December 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 14	Ensure that a general support system security plan is prepared, and kept current, which addresses all of the requirements of OMB Circular A-130 for each general support system identified.

Agency Response

FSIS stated that it will prepare a security plan that addresses all the required and relevant elements specified by OMB Circular A-130. The plan will be prepared by rank order of priority for the general support systems. For the general support systems identified in recommendation No. 14, FSIS will identify the individuals responsible for security for each system, certify the security of all support systems that maintain sensitive data, and establish contingency plans and recovery procedures in the event of a disaster. The security plan for all support systems will be finalized by June 2004.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 15	Ensure that application security plans are prepared, kept current, and include all elements required by OMB Circular A-130 for each of the major application systems identified.

Agency Response

FSIS stated that it will prepare a security plan that addresses all the required and relevant elements specified by OMB Circular A-130. For the application systems, FSIS will identify the individuals responsible for security for each system, certify the security of all application systems that maintain sensitive data, and establish contingency plans and recovery procedures in the event of a disaster. The security plan for all major application systems will be finalized by June 2004.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 16	Establish controls to ensure that an independent review of security controls is conducted for each major application at least every 3 years and certify the application as required.

Agency Response

FSIS stated that it will review the security controls for each major application at least every three years. FSIS will review a third of the major applications each year in order to ensure that all applications have been reviewed during the three-year cycle. AISD will certify or obtain the certification of the major applications. The review process will be developed and incorporated into the annual management control reviews by December 2003.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 17	Ensure that each major application has been authorized for processing by the management official responsible for the application.

Agency Response

FSIS stated that it will ensure that each major application has been authorized for processing by having the responsible management official sign an accreditation document. The applications will be certified prior to being accredited. All major applications will be accredited by June 2003.

OIG Position

Management decision has been reached on this recommendation.

FINDING NO. 5 FSIS NEEDS TO DEVELOP AND IMPLEMENT A DISASTER RECOVERY/ BUSINESS CONTINUITY PLAN	FSIS had not developed a formal plan to ensure the recovery and continuity of operations in the event of a disaster. FSIS officials recognized the need to prepare plans to address business continuity, but officials informed us that this task had yet to be a priority. FSIS officials further cited a lack of personnel and other resources to complete these plans. As a result, FSIS cannot be assured that it can quickly and effectively resume operations in the event of a disaster or other service disruption.

Contingency planning directly supports an organization's goal of continued operations and addresses how to keep an organization's critical functions

operating in the event of disruptions, both large and small. NIST issued "Generally Accepted Principles and Practices for Securing Information Technology Systems" in September 1996, which identified five steps describing the basic functions an organization should employ when developing contingency plans. These five steps include: (1) Developing a Business Plan; (2) Identifying Needed Resources; (3) Developing Scenarios; (4) Developing Strategies; and (5) Testing and Revising the Plan.

OMB[4] provides minimum controls to be included in Federal automated information security programs. Under "Continuity of Support" it states: "Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system."

FSIS does not have a disaster recovery plan in place. Furthermore, none of the FSIS security plans we reviewed adequately addressed business continuity and contingency planning to ensure the continuity of operations in the event of a disaster or an interruption in services. The security plans only addressed the various backup routines in place for backing up the files and data stored on the various servers throughout FSIS.

Our review of the general support system security plan for the FSIS Enterprise Network also disclosed inadequate contingency planning. While this security plan stated that a contingency plan was 'in place,' and did describe the availability of back up hardware, the hardware described in the security plan is no longer in use.

Finally, our review of the general support system security plan prepared for FSIS' FPC, located in Iowa and which processes field payroll and other payments, disclosed that contingency planning was again limited to a general discussion of the backup procedures in place for the local file systems. However, it did not address alternate processing sites or the types of disasters, which could impact on local operations. This security plan had identified the sensitivity of the data being processed at the site as "high" in regards to confidentiality, integrity, and availability. Further, FSIS had not prepared a contingency plan for its TSC which serves as FSIS' center for technical assistance for field employees, processing plants, and trade and consumer groups.

The USDA Office of Chief Information Office (OCIO) reviewed the FSIS FY 2001 Annual Information Security Plan as part of its review under the Government Information Security Reform Act of 2000. The OCIO

[4] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000.

recommended that FSIS "Fund and commit resources, based upon the Risk Analysis, to the development of an executable disaster recovery plan for their mission critical systems."

RECOMMENDATION NO. 18

Prepare and periodically update comprehensive and system specific contingency plans that address protection of information resources and recovery procedures, including the offsite storage requirements, in the event of service disruptions. Include a description of these plans in each sites' security plans.

Agency Response

FSIS stated that it is in the process of creating a backup facility and preparing system contingency plans that address protection of information resources and recovery procedures, including offsite storage requirements, in the event of service disruptions. A description of these plans will be included in each site's security plan. The system specific contingency plan will be completed by June 2004.

OIG Position

Management decision has been reached on this recommendation.

FINDING NO. 6

FSIS NEEDS TO ESTABLISH A SYSTEM DEVLEOPEMENT LIFECYCLE AND CHANGE CONTROL PROCESSES

FSIS had not implemented a standard system development life cycle (SDLC) process for managing its application development and change control process. FSIS does not maintain formal project plans, change control forms, approvals, test plans, or testing results. FSIS officials agreed that a standard SDLC was not in place, but said that funding had not been approved that would allow them to establish a formal SDLC. We also reported FSIS' lack of adequate testing and documentation of testing results in Audit Report No. 50099-21-FM, "*Review of the Year 2000 Conversion Process - Validation Phase*," issued in September 1999. Without a formal SDLC process and adequate documentation, it is not possible to assess whether systems under development and systems undergoing modification are properly approved, contain all needed security features, and are properly authorized before modifications are made.

FSIS Directive 1300.1, "FSIS Information Resources Management," dated April 5, 1994, states that Automated Information Systems Division has been assigned the responsibility to provide leadership and staff or contractor support of multiple office system development or enhancement projects. Support includes analysis, design, programming, testing, documenting, and training. Systems development efforts must follow system life cycle management practices and use structured techniques. DMs 3200-1 and 3200-2, "Application Systems Life Cycle Management," and "A Project Manager's Guide to Application Systems Life Cycle Management," respectively, both dated March 3, 1988, provide detailed guidance for managing application system development projects and identifies the various documentation that should accompany each phase of the projects' life cycle.

FSIS is currently in the process of making major as well as minor modifications to eight of its nine major applications. FSIS personnel said their system development and modification process is accomplished through a committee that discusses what needs to be developed or what needs to be changed. These discussions are held through conference calls and through e-mails. There are no formal project plans, change control forms, test plans and results, or specific management approval documents prepared for the projects. We did find that project plans and test plans had been prepared for some of the non-major application development efforts; however, one FSIS official stated they did not have the time or resources to comply with an SDLC during major application development or modification.

The lack of adequate testing documentation during system modifications was previously reported in Audit Report No. 50099-21-FM, "Review of the Year 2000 Conversion Process – Validation Phase," issued in September 1999. At that time, we reported that the testing documentation to ensure Year 2000 compliancy was "...insufficient to ascertain whether the testing was satisfactory." This same condition continues to exist.

RECOMMENDATION NO. 19

Adopt and follow a standard SDLC process for all major applications being developed or modified, including full documentation requirements. A formal but less-stringent SDLC process should be developed and followed for non-major applications.

Agency Response

FSIS stated that it will document the System Development Life Cycle (SDLC) currently being used. The SDLC will be used on all major system

development and modifications. A standard SDLC, in accordance with Department requirements, will be adopted by December 2003 and used on all major system development and modifications. The SDLC will include: a security study, feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post implementation review.

OIG Position

Management decision has been reached on this recommendation.

EXHIBIT A – AUDITEE RESPONSE TO DRAFT REPORT

United States Department of Agriculture | Food Safety and Inspection Service | Washington, D.C. 20250

TO: Richard D. Long
Assistant Inspector General for Audit
Office of Inspector General

JUL 23 2003

FROM: Dr. Garry L. McKee
Administrator
Linda Swacina for

SUBJECT: Office of Inspector General (OIG) Official Draft Report – Security Over the Information Technology Resources at the Food Safety and Inspection Service, Report No. 24099-1-FM

We appreciate the opportunity to review and comment on the subject report. The Food Safety and Inspection Service (FSIS) generally agrees with the report's findings and recommendations, however, we believe that the Agency has sufficiently implemented a number of cost-effective measures to assure the integrity and security of the Agency's support systems and applications.

FSIS has outlined a number of positive actions that it has taken or plans to take to respond to the report's recommendations. A secure information technology (IT) infrastructure is very important. Further, FSIS is committed to improving its IT infrastructure in order to meet the current and emerging IT security requirements. The Agency's responses to this report further document the actions taken to improve the IT security. Many of the Agency's long-term corrective actions will be dependent upon available funding.

Chapter 1. Vulnerabilities Expose FSIS' Systems to the Risk of Malicious Attacks

1. **Recommendation No. 1**
Ensure all necessary corrective actions are completed on all high and medium risk vulnerabilities identified during our audit.

Agency Response
FSIS has completed corrective actions on all 6 high risk vulnerabilities identified during the audit. Action was also completed on 62 of the 73 medium vulnerabilities, with 11 still unresolved. The Agency's progress in addressing the vulnerabilities is evident when a comparison is made between the original scan report and a recent scan. Enclosure No. 1 contains a recent scan report for the FSIS information systems; however, this scan report shows new vulnerabilities that are not pertinent to the OIG report. The Agency will institute fixes for the remaining 11 unresolved medium vulnerabilities. A report detailing the Agency's corrective actions to resolve these 11 will be prepared by September 2003.

FSIS FORM 2630-9 (6/96) EQUAL OPPORTUNITY IN EMPLOYMENT AND SERVICES

2. **Recommendation No. 2**
Develop a formal process for conducting security scans of the servers and network equipment that include procedures to ensure vulnerabilities are reviewed and that corrective actions are documented.

Agency Response
FSIS has instituted bi-weekly [redacted] inspections. The scans allow FSIS IT personnel to regularly perform audits and assess the network parameters and stay cognizant of any potential security misconfigurations and anomalies. The bi-weekly inspections allow FSIS to take the necessary corrective actions before the network is compromised. Patches that are approved for use on FSIS operating systems and applications are usually implemented within three weeks after the scan dates. Patches that cannot be applied will be documented as to why they were not approved and installed.

Additionally, FSIS purchased an intrusion prevention software package to help protect the integrity of FSIS' applications and operating systems. The StormWatch software proactively protects enterprises against known and unknown security risks. Unlike existing FSIS security solutions that are attack-centric and reliant on databases of known attack signatures, StormWatch is application-centric, focusing on the behavior of FSIS critical computer applications.

3. **Recommendation No. 3**
Ensure that the ongoing process of installing firewall security is timely completed.

Agency Response
FSIS is in the process of implementing firewall security. FSIS will establish controls to periodically review the firewall configuration to ensure that this is kept current and that user accounts on the firewall system are kept to a minimum and are properly disabled or removed when not needed. FSIS will complete the firewall security installation by December 2003.

Chapter 2. FSIS Needs to Improve the Physical and Logical Access Controls Over its Network and Critical Databases

4. **Recommendation No. 4**
Develop a formal process for granting physical access to the HQ computer facility that includes requiring the completion of an access request form identifying the reason the access is needed and requiring supervisory approval of the need.

Agency Response
FSIS will develop a formal process for granting access to the HQ computer facility that includes requiring the completion of an access request form identifying the reason the access is needed and requiring supervisory approval of the need. The written process will include the procedures for authorizing

approval for access to the HQ computer facility. The form will provide a general description of the grantee's work function requiring access to the computer facility. For efficiency, a single form will be used to cover continuing activities that require recurring access to the facility. FSIS will complete the development of the formal process and form by December 2003.

5. **Recommendation No. 5**
Ensure that only employees who need access to the computer room for the performance of their duties are allowed unrestricted access.

Agency Response
FSIS is in the process of removing and relocating spare equipment that was being stored in the computer facility to a separate secure location to limit access to the computer facility. In addition, FSIS will install a card key access system that will track individuals entering the computer facility. Only employees requiring access to the computer room for the performance of their duties will be allowed unrestricted access. Funds for the card key system have been committed and FSIS is making arrangements with the Department to proceed with the work. FSIS expects the new system to be operational by December 2003.

6. **Recommendation No. 6**
Take action to ensure that the computer room access door hinges are adequately secured.

Agency Response
FSIS has pinned the door hinges to secure them and prevent unauthorized entrance into the computer room. Three holes were drilled within the internal side of the door hinges and safety studs were inserted and welded in place to prevent removal of the hinges. Enclosure No. 2 contains a copy of the work order for this completed work.

7. **Recommendation No. 7**
Update the security plan for the computer facility to reflect the current operating environment and to address all the required security actions.

Agency Response
FSIS will update the security plan for the computer facility. The plan will identify security actions required to maintain an adequate computer room environment. FSIS expects to have an updated security plan by May 2004.

8. **Recommendation No. 8**
Develop and document procedures for performing tape backups that includes maintaining an inventory of tapes at the offsite storage facility and a standard tape labeling process

Agency Response
FSIS will develop procedures for performing tape backups that includes maintaining an inventory of tapes at the offsite storage facility. The procedures will also include a process for labeling the backup tapes. FSIS will issue the procedures by May 2004.

9. **Recommendation No. 9**
Ensure that personnel responsible for assigning and maintaining user access to the major applications are routinely provided a list of separated employees.

Agency Response
FSIS makes a concerted effort to remove separated user accounts in a timely manner. FSIS distributes to key managers a personnel list that provides information on employees that have been recently hired, separated, and transferred. Starting in July 2003, the Automated Information System Division (AISD) will be provided with a bi-monthly list of separated or transferred employees by the Human Resources Division. The AISD personnel responsible for assigning and maintaining user access to the major applications will be provided with the list. FSIS will close user accounts of employees who no longer require access to the network within two business day of receipt of listing.

10. **Recommendation No. 10**
Assign responsibilities for review of the security event history logs for all major applications and network, and identify the specific security events to be filtered for review.

Agency Response
FSIS is currently using support contractors to carry out its responsibilities for tracking the security and activity related events and storing them in a security event history log. FSIS will develop written procedures covering the process that the system administrators will use to review the security history log. The procedures will also identify the specific activity events to be filtered for review. The procedures will be developed by December 2003.

11. **Recommendation No. 11**
Develop a formal process to ensure that only authorized changes are made to database data. Ensure the process requires full documentation of the need for the change and management approval and review of the change.

Agency Response
FSIS has established a Change Control Board (CCB) to oversee system changes. The CCB has the responsibility to review and approve all system and database changes. The CCB has been functioning since May 2003. The CCB Chair is responsible for ensuring that all database system changes are documented. Enclosure No. 3 contains a charter for the CCB.

FSIS will document the formal process that the CCB uses to ensure that only authorized changes are made to the database data. The formal process will be issued by December 2003.

12. **Recommendation No. 12**
Review the access authorities granted to the 22 individuals with database administration (DBA) authority. Document these individuals need for this level of access, or remove the privilege.

Agency Response
FSIS will review the access authorities of the 22 individuals granted DBA authority. The Agency will verify that these individuals have a legitimate need for having this level of authority or remove this privilege. FSIS will complete this determination and documentation by September 2003.

Chapter 3. FSIS Needs to Ensure Compliance with Existing Federal Information Security Requirements

13. **Recommendation No. 13**
Perform an assessment to identify each of the general support systems within FSIS.

Agency Response
FSIS will identify relevant criteria and identify each of the general support systems within FSIS by December 2003.

14. **Recommendation No. 14**
Ensure that a general support system security plan is prepared, and kept current, which addresses all of the requirements of OMB Circular A-130 for each general support system identified.

Agency Response
FSIS will prepare a security plan that addresses all the required and relevant elements specified by OMB Circular A-130. The plan will be prepared by rank order of priority for the general support systems. For the general support systems identified in recommendation No. 14, FSIS will identify the individuals responsible for security for each system, certify the security of all support systems that maintain sensitive data, and establish contingency plans and recovery procedures in the event of a disaster. The security plan for all support systems will be finalized by June 2004.

15. **Recommendation No. 15**
Ensure that application security plans are prepared, kept current, and include all elements required by OMB Circular A-130 for each of the major application systems identified.

Agency Response
FSIS will prepare a security plan that addresses all the required and relevant elements specified by OMB Circular A-130. For the application systems, FSIS will identify the individuals responsible for security for each system, certify the security of all application systems that maintain sensitive data, and establish contingency plans and recovery procedures in the event of a disaster. The security plan for all major application systems will be finalized by June 2004.

16. **Recommendation No. 16**
Establish controls to ensure that an independent review of security controls is conducted for each major application at least every 3 years and certify the application as required.

Agency Response
FSIS will review the security controls for each major application at least every three years. FSIS will review a third of the major applications each year in order to ensure that all applications have been reviewed during the three year cycle. AISD will certify or obtain the certification of the major applications. The review process will be developed and incorporated into the annual management control reviews by December 2003.

17. **Recommendation No. 17**
Ensure that each major application has been authorized for processing by the management official responsible for the application.

Agency Response
FSIS will ensure that each major application has been authorized for processing by having the responsible management official sign an accreditation document. The applications will be certified prior to being accredited. All major applications will be accredited by June 2003.

18. **Recommendation No. 18**
Prepare and periodically update comprehensive and system specific contingency plans that address protection of information resources and recovery procedures, including the offsite storage requirements, in the event of service disruptions. Include a description of these plans in each sites' security plans.

Agency Response
FSIS is in the process of creating a backup facility and preparing system contingency plans that address protection of information resources and recovery procedures, including offsite storage requirements, in the event of service disruptions. A description of these plans will be included in each site's security plan. The system specific contingency plan will be completed by June 2004.

19. **Recommendation No. 19**
Adopt and follow a standard SDLC process for all applications being developed or modified, including full documentation requirements.

Agency Response
FSIS will document the System Development Life Cycle (SDLC) currently being used. The SDLC will be used on all major system development and modifications. A standard SDLC, in accordance with Department requirements, will be adopted by December 2003 and used on all major system development and modifications. The SDLC will include: a security study, feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post implementation review.

Enclosures (3)

ABBREVIATIONS

DBA	Database Administrator
DM	Departmental Manual
EMC	Electronic Mail Coordinator
FPC	*Financial Processing Center*
FSIS	Food Safety Inspection Service
FY	Fiscal Year
HQ	Headquarters
ID	Identification
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	*Office of the Chief Information Officer*
OMB	Office of Management and Budget
SDLC	System Development Life Cycle
TCP/IP	Transmission Control Protocol/Internet Protocol
TSC	Technical Service Center
USDA	U. S. Department of Agriculture